Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

determining a value of a bit of said scalar value; and

executing operations on said elliptic curve a predetermined number of times and in a predetermined order without depending on said determined value of said bit to calculate a scalar multiplied point;

wherein said operations include calculations of addition and doubling, said operations being selected for a bit value of one or zero, the bit value determining the ~~contents of said~~ addition and doubling calculations to be executed.

2. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

determining a value of a bit of said scalar value; and

executing calculations of addition on said elliptic curve and doubling on said elliptic curve in the order that said doubling on said elliptic curve is executed after said addition on said elliptic curve is executed to calculate a scalar multiplied point;

wherein said addition and doubling calculations are selected for a bit value of one or zero, the bit value determining the ~~contents of said~~ addition and doubling calculations to be executed.

3. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

determining a value of a bit of said scalar value; and

executing calculations of addition on said elliptic curve and doubling on said elliptic curve in the order that said addition on said elliptic curve is executed after said doubling on said elliptic curve is executed to calculate a scalar multiplied point;

wherein said addition and doubling calculations are selected for a bit value of one or zero, the bit value determining the ~~contents of said~~ addition and doubling calculations to be executed.

4. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

determining a value of a bit of said scalar value; and

executing calculations of addition on said elliptic curve and doubling on said elliptic curve simultaneously to calculate a scalar multiplied point;

wherein said addition and doubling calculations are selected for a bit value of one or zero, the bit value determining the ~~contents of said~~ addition and doubling calculations to be executed.

5. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

executing addition on said elliptic curve;

determining a value of a bit of said scalar value; and

executing doubling calculations on said elliptic curve to calculate a scalar multiplied point;

wherein said doubling calculations are selected for a bit value of one or zero, the bit value determining the ~~contents of said~~ doubling calculations to be executed.

6. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve;

determining a value of a bit of said scalar value; and

executing said addition on said elliptic curve and said doubling on said elliptic curve in said order randomized by said step of randomizing calculation order of

addition on said elliptic curve and doubling on said elliptic curve to calculate a scalar multiplied point;

wherein said calculations of addition and doubling are selected for a bit value of one or zero, the bit value determining the ~~contents of said~~ addition and doubling calculations to be executed.

7. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve, comprising the steps of:

determining a value of a bit of said scalar value;

randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve; and

executing said addition on said elliptic curve and said doubling on said elliptic curve in said order randomized by said step of randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve to calculate a scalar multiplied point;

wherein said calculations of addition and doubling are selected for a bit value of one or zero, the bit value determining the ~~selection of said~~ addition and doubling calculations to be executed.

8. (original) A data generation method for generating second data from first data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

9. (original) A signature generation method for generating signature data from data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

10. (original) A decryption method for generating decrypted data from encrypted data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

11. (currently amended) A scalar multiplication calculator for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising:

bit value judgment means for determining a value of a bit of said scalar value;

addition operation means for executing addition calculations on said elliptic curve; and

doubling operation means for executing doubling calculations on said elliptic curve;

wherein after the value of said bit of scalar value is determined by said bit value judgment means, said addition on said elliptic curve and said doubling on said elliptic curve are executed by said addition operation means and said doubling operation means a predetermined number of times and in a predetermined order so as to calculate a scalar multiplied point,

wherein said addition and doubling calculations are selected for a bit value of one or zero, the bit value determining the ~~selection of said~~ addition and doubling calculations to be executed.

12. (original) A recording medium for storing a program relating to a scalar multiplication calculation method according to any one of Claims 1 to 7.

13. (original) A scalar multiplication calculation method according to any one of Claims 1 to 7, wherein a Montgomery-form elliptic curve is used as said elliptic curve.

14. (original) A scalar multiplication calculation method according to any one of Claims 1 to 7, wherein an elliptic curve defined on a finite field of characteristic 2 is used as said elliptic curve.

15. (currently amended) The multiplication calculation method according to claim 1, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling

calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

16. (currently amended) The multiplication calculation method according to claim 2, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

17. (currently amended) The multiplication calculation method according to claim 3, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

18. (currently amended) The multiplication calculation method according to claim 4, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

19. (currently amended) The multiplication calculation method according to claim 5, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

20. (currently amended) The multiplication calculation method according to claim 6, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling

calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

21. (currently amended) The multiplication calculation method according to claim 7, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

22. (currently amended) The multiplication calculation method according to claim 11, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a point (m+1)P and the doubling calculations include doubling the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.